CLAIMS

I/we claim:

[c1] 1. A method for synchronizing a cryptosystem in a wireless communication system, the method comprising:

processing a message for transmission, wherein the message includes control data and payload data, and wherein the control data is not encrypted;

determining whether the control data contains a particular control message;

if the control data contains the particular control message, loading an encryption synchronization counter with a number of control message bytes to be transmitted and initializing the encryption synchronization counter;

when the encryption synchronization counter is decremented to zero, indicating that the entire message has been transmitted, initializing the cryptosystem using a key;

using the cryptosystem to encrypt the message;

creating an encrypted airlink packet for transmission over an airlink;

receiving an encrypted message, including control data and payload data, over the airlink;

parsing the message to separate the control data from the payload data;

determining whether the control data contains the particular control message;

if the control data contains the particular control message, initializing the cryptosystem using the key; and

using the cryptosystem to decrypt the message.

[c2] 2. The method of claim 1, wherein the particular control message is a final link control channel ("LCC") message transmitted before the transmission of payload data begins, and wherein transmission of the final link control channel occurs each time a call over an airlink channel is set up.

[c3] 3. The method of claim 1, wherein initializing the cryptosystem includes operating on a state box using the key.

[c4] 4. The method of claim 1, wherein initializing the cryptosystem comprises:

performing a mathematical operation on the key to alter the key for security, wherein the key is an array of data; and

operating on a state box using the altered key, wherein the state box is an array of data.

[c5] 5. The method of claim 1, wherein the cryptosystem includes an RC4 state box and an RC4 key, and wherein the payload data is operated on using the RC4 state box for encryption and decryption.

[c6] 6. A method for synchronizing a cryptosystem between a sender and a receiver in a wireless network comprising at least one base station and at least one remote unit, the method comprising:

detecting a particular control message at an associated control channel ("ACC") level that is sent each time an airlink channel is set up; and

in response to detecting the particular control message, determining a point in the transmission at which to begin operating the cryptosystem, including changing an encryption key that is used by the base station and the remote unit.

[c7] 7. The method of claim 6, wherein the particular control message is a final control message sent before payload data is sent

[c8] 8. The method of claim 6, further comprising using the changed encryption key to generate a state box that is used by the base station and the remote unit to perform encryption and decryption.

[c9] 9. The method of claim 6, wherein the operation of the cryptosystem occurs at the ACC level.

[c10] 10. The method of claim 6, further comprising:

loading an encryption synchronization counter with a size of an ACC message that contains the particular control message, wherein the ACC message is transmitted in blocks;

decrementing the encryption synchronization counter to zero when a last block of the ACC message has been transmitted; and

when the particular control message has been detected and the encryption synchronization counter is zero, initializing the cryptosystem.

[c11] 11. The method of claim 6, wherein the particular control message is either a "set asynchronous balance mode" ("SABM") message or a "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") message.

[c12] 12. The method of claim 6, wherein the cryptosystem includes an RC4 state box that is generated by the encryption key.

[c13] 13. A wireless communication system, comprising:

at least one remote unit comprising,

at least one digital signal processor ("DSP");

a central processing unit; and

a memory device, wherein the at least one remote unit is configured to receive data from and send data to at least one base station; and

at least one base station comprising,

at least one DSP;

a central processing unit; and

a memory device, wherein the at least one base station is configured to detect a particular control message in a data transmission and, in response, initiate an encryption/decryption process, wherein the particular control message is an associated control channel ("ACC") message that occurs just before the transmission of telephony data.

[c14] 14. The system of claim 13, wherein initiating the encryption decryption process includes the base station transmitting an encryption key via a traffic channel request message, and wherein the encryption key is used by the remote unit and the base station to generate a state box.

[c15] 15. The system of claim 13, wherein the at least one DSP of the base station comprises an airlink DSP including a memory that contains a software architecture, the software architecture comprising:

an ACC function module; and

a traffic channel ("TCH") function module, wherein initiating the encryption/decryption process includes the ACC function module and the TCH function module accessing an encryption/decryption function module to prepare an encryption key and begin the encryption/decryption process using an encryption/decryption algorithm.

[c16] 16. The system of claim 15, wherein the encryption/decryption algorithm is an RC4 algorithm.

[c17] 17. The system of claim 13, wherein the particular control message is selected from a group comprising a "set asynchronous balance mode" ("SABM") message and a "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") message.

[c18] 18. A computer-readable medium whose contents cause a transmitter in a communications system to perform a method for synchronizing encryption/decryption of transmitted data, the method comprising creating a packet for transmission over a link, including:

sending messages in blocks of data from a central processing unit ("CPU") to a communication link digital signal processor;

detecting a particular control message in the blocks of data;

in response to detecting, loading a size of a message into a counter, wherein the counter reaches zero when all of the blocks in the message have been sent;

when the counter reaches zero, initiating an encryption/decryption synchronization process, including generating a state box using an encryption key; and

encrypting transmissions following the message for the packet.

[c19] 19. The computer readable medium of claim 18, wherein the method further comprises creating a control message packet for sending to the CPU, including,

receiving an airlink packet;

parsing the airlink packet to separate payload data from control data;

detecting a particular control message in the airlink packet;

in response to detecting, initiating an encryption/decryption synchronization process, including generating a state box using an encryption key; and

decrypting data following the particular control message.

[c20] 20. The computer readable medium of claim 18, wherein the packet comprises the encryption key.

[c21] 21. The computer readable medium of claim 18, wherein initiating the encryption/decryption synchronization process further includes changing the encryption key according to a predetermined algorithm, and operating on the state box using the changed encryption key.

[c22] 22. The computer readable medium of claim 18, wherein the method is performed at an associated control channel level of processing.

[c23] 23. The computer readable medium of claim 18, wherein the method is performed each time the base station participates in setting up an airlink channel.

[c24] 24. The computer readable medium of claim 18, wherein the particular control message is a link control channel ("LCC") message that is a "set asynchronous balance mode" ("SABM") message and a "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") message.

[c25] 25. An apparatus for synchronizing an encryption /decryption process in a wireless communication network, comprising:

at least one digital signal processing means;

at least one central processing means; and

encryption synchronization means configured to detect a particular control message in a data transmission and, in response, initiate an encryption/decryption process, wherein the particular control message occurs just before the transmission of telephony data.

[c26] 26. The apparatus of claim 25, wherein the encryption synchronization means is further configured to provide a current encryption key to receiving devices and sending devices in the wireless communication network.

[c27] 27. The apparatus of claim 25, wherein the encryption synchronization means is further configured to count data blocks in a message being transmitted to determine when to begin encryption/decryption.

[c28] 28. The apparatus of claim 26, wherein initiating the encryption/decryption process comprises using the current encryption key to generate a current state box, wherein the current state box is used to operate on the telephony data.

[c29] 29. The apparatus of claim 25, wherein the encryption synchronization means and the encryption/decryption process operates at an associated control channel level in the wireless communication network.

[c30] 30. The apparatus of claim 25, wherein the initiation of the encryption/decryption process occurs each time a wireless connection is set up, comprising initial connection, connection hand off, and connection reestablishment after unexpected connection loss.

[c31] 31. A cryptographic method, comprising:

detecting a particular trigger upon establishment of a wireless telephony communication link between at least one wireless transmitter and one wireless receiver, wherein the communication link is established under at least one known wireless protocol, and wherein the particular trigger is at a know time or location under the communication link establishment of the known wireless protocol; and

in response to detecting the particular trigger, determining a point in the transmission at which to begin applying a stream cipher.

[c32] 32. The method of claim 31, wherein the particular trigger is either a "set asynchronous balance mode" ("SABM") message or a "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") message sent at an associated control channel ("ACC") level each time an airlink channel is established.

[c33] 33. A method of synchronizing an encryption data array at a transmitter to a decryption data array at receiver in a wireless communication network, the method comprising:

establishing a call between the transmitter and the receiver using a call establishment message transmitted from the transmitter to the receiver;

parsing the call establishment message to produce a parsed call establishment message;

determining an encryption state of the transmitter based on the parsed call establishment message; and

synchronizing the decryption data array at the receiver based to the encryption data array at the transmitter based on the encryption state of the transmitter.